*i*Government
Working Paper Series

The *i*Government working paper series discusses the broad issues surrounding information, knowledge, information systems, and information and communication technologies in the public sector

Paper No. 21

A Framework for Assessing Privacy Readiness of e-Government

KRISTOF KESSLER, NILS HETTICH, CHADLEY PARSONS, CRAIG RICHARDSON & ANNY TRIANA

2011

ISBN: 978-1-905469-15-4

Published by: ***Centre for Development Informatics***
Institute for Development Policy and Management, SED
University of Manchester, Arthur Lewis Building, Manchester, M13 9PL, UK
Tel: +44-161-275-2804 Email: cdi@manchester.ac.uk
Web: http://www.manchester.ac.uk/cdi

View/Download from:
http://www.sed.manchester.ac.uk/idpm/research/publications/wp/igovernment/index.htm

Educators' Guide from:
http://www.sed.manchester.ac.uk/idpm/research/publications/wp/igovernment/educigov.htm

Table of Contents

A Framework for Assessing Privacy Readiness of e-Government

Kristof Kessler, Nils Hettich,
Chadley Parsons, Craig Richardson & Anny Triana
Centre for Development Informatics
IDPM, University of Manchester, UK
2011

Abstract

While rapid growth of information and communication technology in government can facilitate improved service provision, it can also pose a privacy threat. Privacy is thus a key concern in the establishment – and the success or failure – of e-government systems. Yet research into privacy requirements related to e-government has not so far yielded an appropriate analytical framework. Consequently, the purpose of this paper is to develop such a framework.

The proposed framework incorporates the five maturity stages of e-government and their specific privacy requirements from a *Policy*, *Technology* and *Citizen* requirements perspective. Its utilization and implications are then outlined by analysing and comparing two case examples; one from Germany, one from Kenya. Researchers and practitioners can use the proposed framework to identify major privacy-related issues in citizen-facing e-government systems and to develop appropriate recommendations for action.

A. Introduction

A1. Challenges for Successful e-Government

Rapid growth of information and communication technologies (ICTs) in government has enabled significant amounts of information to be stored about citizens. The efficiency of electronic data management facilitates integrated citizen information, but also introduces complex requirements for controls and processes. As the use and integration of these technologies proliferate, the potential negative consequences for citizens increase. Intrusive data collection, misuse of personal information and constant surveillance are common fears. Given that the state is the largest single collector of citizen information, the potential for these fears to become reality is not entirely misguided.

Reviewing these assertions more closely, a correlation between the amount of data collected and the technology integration period of e-government can be established as outlined in Figure 1. From a historical perspective, the growth of data collection in governmental processes can be separated into three technology integration periods: sparseness, maturity and ambiance (Holvast, 2009). Up until the 1980s use of information technology in governmental processes was sparse and disconnected. Data collection was present and already controversial, but far less comprehensive than in the period to follow. Furthermore, it was limited by physical boundaries dictated by paper-based systems or sparse and expensive technology. The explosive technological and scientific developments from the 1980s to the present day led to a proliferation of mature technologies; spurring growth in data collection. In particular, interconnecting, telecommunicating, storing and querying different types of personal and sensitive data was made possible at a far higher comprehensiveness with or without knowledge of a

respective individual. This resulted in an exponential growth in data collection and hence in the importance of privacy. In the foreseeable future, new technologies, such as grid technology and ubiquitous computing, will not only transform e-government into m-government but beyond this into a ubiquitous u-government (El Kiki and Lawrence, 2006). This will result in an even stronger growth in data collection due to the use of technology pervading nearly every aspect of human life.

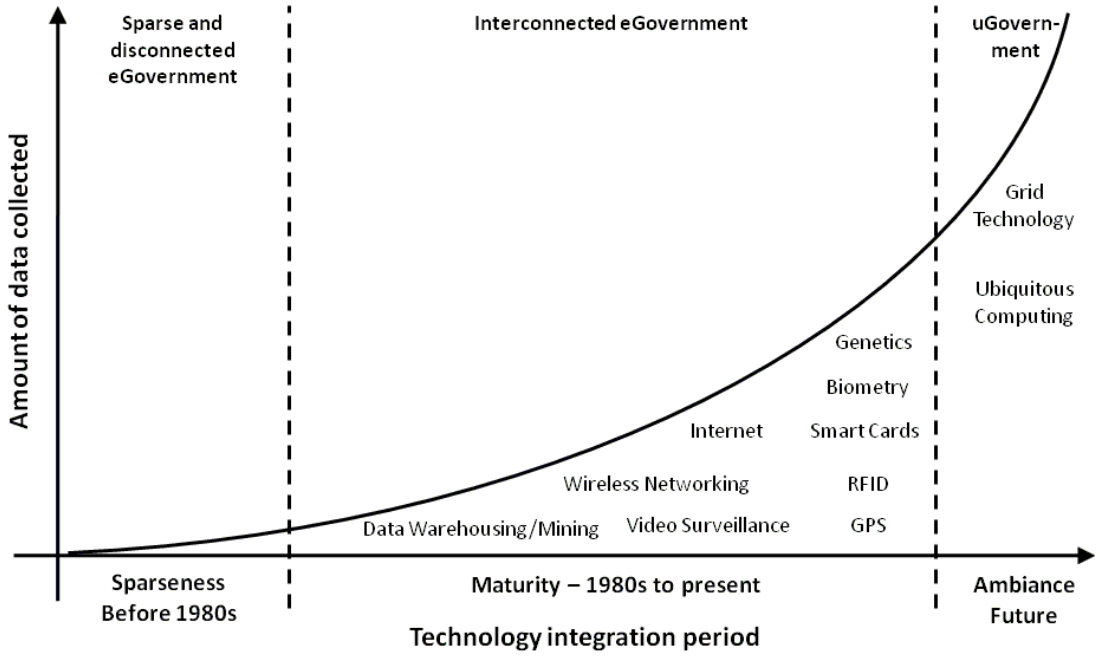

Figure 1: Relationship between Data Collection and Technology Integration Period of e-Government

Sources: Developed from El Kiki and Lawrence (2006), and Holvast (2009)

A2. The Concept of Privacy

Definitions of privacy cover a variety of perspectives. Amalgamating these, privacy can be defined as the absence of unreasonable, and potentially intrusive, collection and use of personal information (Langenderfer and Miyazaki, 2009; Laudon and Laudon, 2009; LaRose and Rifon, 2007; Culnan, 2000). As Choudrie et al. (2009) have pointed out, privacy is more of a social consideration, while security is more of a technical consideration. It is therefore important to discuss the overlapping implications for citizens of e-government. As an example, identity theft due to

security and privacy breaches is a growing type of white-collar criminal activity. According to a Federal Trade Commission estimate in 2003, "almost 10 million Americans have discovered that they were the victim of some form of ID theft within the past year" (Solove, 2004). This identity theft can lead to financial theft, coercion and other privacy risks. In his acclaimed novel "1984", George Orwell (1949) envisioned a totalitarian state, which uses citizens' personal information for absolute suppression. Although unrealistic in some respects, it does resonate with the potential misuses of citizen information.

The actions and failures of existing oppressive states exemplify the potential vulnerability they may beset citizens. While this vulnerability can be exploited by individuals or criminal gangs, it is suggested that the potential negative consequences of abuse of citizens' privacy by governments will impact a larger number of citizens and with more severe consequences. Through the unreasonable collection and exploitation of personal information the state could suppress basic human rights and liberties. Whichever the particular agent, all this leads to the necessity to critically analyse the state's e-government systems to derive implications regarding privacy risks, make recommendations for privacy protection, and encourage citizen adoption. For this purpose this paper outlines a framework for assessing privacy readiness of e-government.

B. Framework for Assessing Privacy Readiness of e-Government

B1. Introduction and Rationale

Reviewing the literature on e-government and privacy, it can be determined that no integrated framework for assessing privacy readiness of e-government is available. Establishing a framework addressing this subject would facilitate academic research as well as knowledge transfer to address practical issues and by this enable a more focused approach. The proposed framework in Figure 2 outlines the factors that are necessary to address the subject of privacy readiness in e-government at different stages of e-government maturity. Three perspectives on e-privacy form the requirements for each stage: *Policy*, *Technology*, and *Citizen*. These three requirement perspectives are based on necessary privacy protection measures in terms of collection

and use limitation as well as purpose specification, security safeguards and individual participation (Holvast, 2009). As e-government progresses through the five maturity stages these requirements must be addressed adequately and simultaneously. Without a similar level of maturity the privacy of citizens is potentially compromised which in turn might lead to a failed e-government project; not least due to citizens' opposition.

The aim of the framework is to analyse the necessary requirements for privacy as a success factor in e-government systems: the privacy readiness of e-government. The development of the framework is based on Symonds (2000), Belanger and Hiller (2006) and Holvast (2009). However, the proposed framework's focus comes largely from a citizen perspective. The horizontal axis of the framework outlines the consecutive stages of e-government implementation while the vertical axis applies the three different privacy requirement perspectives. This results in five successive steps per privacy requirement which build upon their respective predecessor indicated by their stair-like alignment within the framework.

Stage of e-Government

Privacy requirement	1 Information	2 Two-way communication	3 Transaction	4 Integration	5 Participation
Policy	Policy on information collection	Policy on information use	Policy on information protection	Policy on information sharing	Policy on informational self-determination
Technology	Appropriate access tracking	Secure communication channel	Integrity of transaction and storage	Data access rights management	Citizen controlled access management
Citizen	Awareness	Trust	Choice (of Transaction)	Consultation	Control

Figure 2: Framework for Assessing Privacy Readiness of e-Government
Sources: developed from Symonds (2000), Belanger and Hiller (2006) and Holvast (2009)

B2. Horizontal Dimension: Maturity Stages

The five maturity stages build upon each other, for example to get to a transactional capability (Stage 3), two-way IT-enabled communication (Stage 2) between government and citizen must be possible. The first four maturity stages are based upon Symonds (2000) to describe a government's evolution in providing electronic services. The first stage, *Information*, recognizes government's initial ability to provide one-way information electronically to citizens. The latter stages progress through *Two-way communication*, e.g. establishing communication via email and online forms, through to citizen centric, integrated electronic service delivery, i.e. *Transaction*, then across multiple departments, *Integration*. The fifth stage, *Participation*, was added by Belanger and Hiller (2006) to reflect government platforms allowing users to participate politically, e.g. by voting or posting comments.

Belanger and Hiller (2006) used this modified framework and mapped privacy issues to each stage from the perspective of policy, law and regulations, technical feasibility and user feasibility. Our review found these requirements to be largely too specific – e.g. outlining the risks in use of internet browser cookies – to have a generalizable application. They were therefore modified at each stage while law and regulation was seen to exist as part of *Policy* for the purpose of this framework. While Holvast (2009) does not provide a structured framework, the conceptual perspective was derived and applied to the proposed framework to cover a similar set of dimensions.

Additionally, the *Participation* stage was not included in Belanger and Hiller's (2006) final privacy framework. As this stage reflects a new dimension of user vulnerability that comes with the age of Web 2.0 philosophies of high user empowerment, it has been included in the proposed framework. It sees government empowering citizens with respect to their privacy, and thus having autonomy regarding any vulnerability they perceive.

B3. Vertical Dimension: Privacy Requirements

The proposed framework adopts a multi-perspective approach – *Policy*, *Technology* and *Citizen* – for determining privacy requirements in the individual stages of e-government. According to Holvast (2009), collection of personal data must fulfil privacy protection in terms of collection and use limitation as well as purpose

specification, security safeguards and individual participation. To address these requirements, three things need to be considered alongside each other for enhancing the privacy readiness of e-government: collective instruments i.e. policy requirements; systemic instruments i.e. technical requirements; and instruments of individual empowerment i.e. citizen requirements. Thus, these three perspectives are chosen for the proposed framework.

Policy requirements

The policy perspective, along the *Policy* row, outlines the evolution of scope and clarity of privacy protection through the maturity stages. This begins with the existence of basic policies on information collection. These may restrict what types and amount of data is collected about citizens as well as stipulate the need to inform citizens about this, but policy here does not yet cover the need to address how the collected data is used. This comes into play in the second stage, with policy adding greater protection of citizens' privacy by specifying how data is used when two-way communication occurs. Government accountability comes into play in the third stage as protection of data becomes part of the government's mandate. This is broadened in the fourth stage where policy needs to define how citizen information is shared between government organizations, possibly reaching down to the level of the roles and responsibilities of the information handler. In the Participation stage policies need to stipulate the complete informational self-determination of the citizen by addressing how a citizen can obtain full control over the data the government has collected about her/him and how the government uses this data.

Technology requirements

With the *Technology* perspective, Belanger and Hiller (2006) saw the tracking of cookies as being the primary stage necessary for privacy policy and thus its manifestation in the application of technology. The proposed framework expands this notion to the concept of regulating technology's ability to collect information indiscriminately and without the citizen's knowledge, so that it occurs in an appropriate manner. In the second stage, where two-way communication is relevant, technology such as encryption and secured storage is used to protect interactions between citizen and e-government system. The third stage additionally requires

systems capable of performing secure and complete transactions, further strengthening the lifecycle of systemized data. Such control can be operationalized and formalized through data access rights management, as defined in the fourth stage. Through this measure access to information is granted or denied based on role, identity, and policies at a potentially high degree of granularity. In the fifth stage, technology put into place by government allows citizens to define which government entities have access to which of their personal data, in consequence allowing for informational self-determination.

Citizen requirements

The *Citizen* perspective has been generalized from the work of Belanger and Hiller (2006) to convey important citizen characteristics which support the advancement of privacy in e-government. These characteristics must be developed through government policy, and practice including the use of technology. Citizen awareness of privacy issues, and the government's policy towards it, forms the basis for the citizen's stake in e-government privacy. In the second stage, this knowledge and the subsequent uptake of e-government systems is supported by citizen trust. Once trust by citizens in the e-government system has been established, the choice of whether to carry out transactions via an e-government system needs to be addressed in the third stage. In the fourth stage, consulted citizens are educated and empowered to decide on which data the government collects about them and how it is used at a high level of granularity while the fifth stage gives full control over this matter to the citizen.

B4. Summary and Overall Implications

The potential success of e-government systems at each stage of complexity can be shown through the framework as being dependent on meeting a combination of policy, technical, and citizen requirements. The privacy requirements represented by the rows of the matrix intend to illustrate that their combination is key to the success of e-government. As shown in the two following case examples, meeting policy and technical requirements alone does not necessarily lead to such a success. Instead, meeting citizen expectations, supported by policy and technical measures, is also required.

C. Analysis of Case Examples

The two case examples outlined in this chapter show how to use the proposed framework for analysing e-government projects in regards to their privacy readiness. Based on this analysis a comparison of the cases is then made to establish recommendations for improving identified shortcomings (noting that comparison is not a necessity in order to derive recommendations for practice: that can be done by applying the framework to a single e-government system). For the purpose of comparison, a more successful project and a more problematic project have been chosen.

C1. Case Example 1: Germany's Tax Administration System

Introduction

Germany's Comprehensive Tax Administration system serves both businesses and citizens. It features online tax filing and status tracking (Elster, 2010a). As outlined in Figure 3, the system can be identified as being in the transaction stage. The most relevant regulations for this application concern tax data transmission, general privacy, tax data sharing, and the legitimacy of electronic signatures. Transaction security is enabled with the help of an electronic signature provided by the tax authorities. The user has multiple options regarding use and channel. For example, the full tax submission process can occur in any combination of paper-based and electronic means, and different means of identification are accepted. The growing number of users, up to approximately eight million since system introduction in 2000 (Elster, 2010b), also indicates the fulfilment of citizen expectations. In the following sections the individual privacy requirements are assessed in more detail.

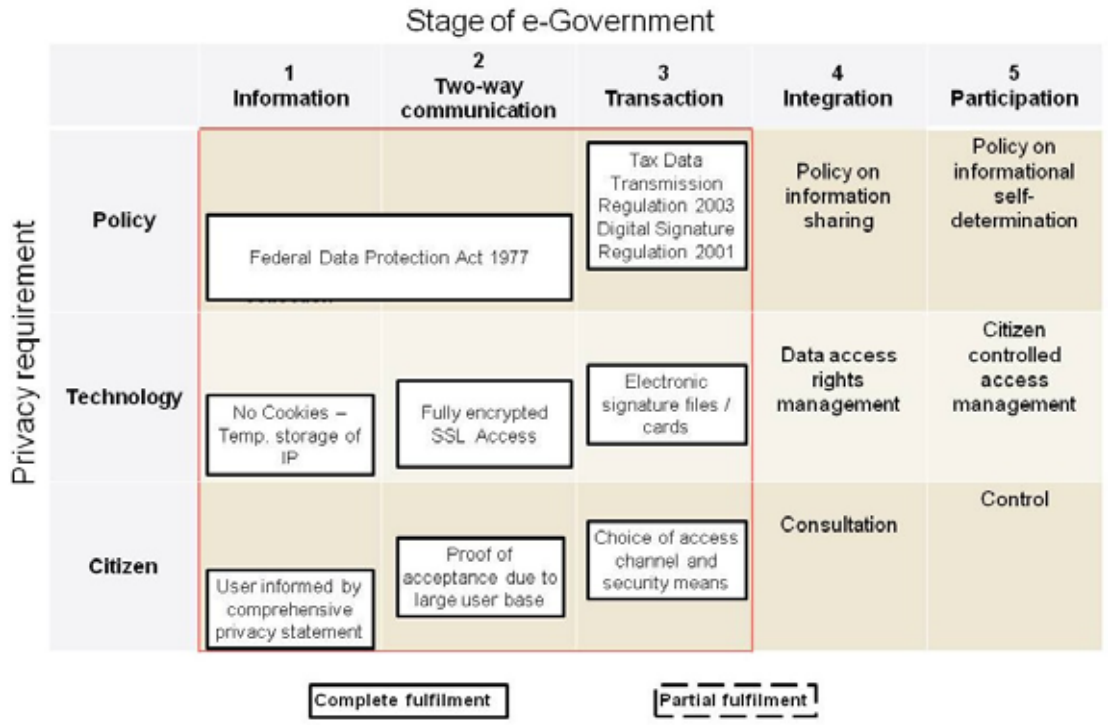

Figure 3: Assessment of Privacy Readiness of Germany's Comprehensive Tax Administration

Policy requirements

A comprehensive set of regulations governs the *Policy* aspects regarding the Comprehensive Tax Administration system for the first three maturity stages of e-government. Policies on information collection and use are stipulated by Germany's Federal Data Protection Act ('Bundesdatenschutzgesetz') of 1977 which outlines that users have to be informed which data about them and their actions is collected and how it is used. This mainly relates to the web portal of the Comprehensive Tax Administration system on which it is clearly stated what information is collected and for which purposes it is used. The transactional stage is governed by the Digital Signature Regulation ('Signaturgesetz') of 2001 and the Tax Data Transmission Regulation ('Steuerdaten-Übermittlungsverordnung') of 2003. These regulations on the one hand permit electronic tax filing and on the other hand outline how the filing procedure is secured by means of digital signatures and encryption. Hence, the existing regulations at least support the first three stages of e-government from a policy perspective.

Technology requirements

From a *Technology* perspective the software and hardware measures in place at least enable a secured and authenticated transaction while information collection is minimized. Hence these measures support the first three stages of e-government. Information collection about visitors to the Comprehensive Tax Administration system's web portal is limited to non-personal items necessary for permitting analysis of technical issues and security. It is at least stated that this information is only stored temporarily (Elster, 2010c). No data, such as browser cookies, is stored on the visitor's computer. Beyond information retrieval from the web platform, two-way communication between the user and the authorities via this platform is fully encrypted via SSL. Enabling transactional security under different circumstances, tax authorities provide different means for authentication by means of digital signatures such as encryption files, USB sticks and signature cards. These technical measures have been ISO 27001-certified by the Federal Office of Information and Security (2009) and hence it can be assumed that they fulfil high standards for information security controls and management.

Citizen requirements

From the *Citizen* requirement perspective it can be suggested that awareness, trust and choice are met and hence the first three maturity stages of e-government are supported. Users visiting the Comprehensive Tax Administration system's web portal are made aware of which information is collected about them by a privacy statement (Elster, 2010c). Citizen's trust in two-way communication extending to transactions with the tax authorities is evidenced by the high and growing number of tax filings via this system since its introduction in the year 2000 (Elster, 2010b). Although the system aims to be the sole channel for tax filing in future, citizens have the choice on whether to use it at all and if so on how to use it. Secure interfaces are available for certified third-party software which allows citizens to choose from a variety of software products for tax filing according to their needs. Paper-based filing in full or partially is still an option, although incentives in the form of quicker turn-around times are granted for electronic filing.

C2. Case Example 2: Kenya's e-Government Portal

Introduction

Our second case example outlines Kenya's policy, its e-government portal, and political factors to understand its potential for electronic privacy based on the *Policy*, *Technology* and *Citizen* requirements of the proposed framework. The e-government offerings analysed for this case are available through Kenya's e-government portal. These comprise various services including passport application tracking, national exam results, corruption reporting and online tax services (Kenya, 2010a). Not all of the sub-websites were functional at the time of writing, with some presenting errors. Thus, only some of the sites were reviewed for the analysis below. Some of these applications can be placed in maturity stage 2, while aspects of the Tax Services and Corruption Reporting systems reach stage 3 (Kenya, 2010a). The necessary policies regulating electronic transactions have been enacted. However, the constitution and government actions do not foster trust by citizens due to allowing and implementing restrictive control over media content and delivery (Wanjiku, 2009). The applications only partially fulfil the necessary requirements for technical maturity. Secure communication channels are not guaranteed for all applications. Furthermore, the tax application reveals vulnerabilities regarding access restrictions (Kenya Revenue Authority, 2010). Summarizing the above, Kenya has met policy requirements but may not have met the technical requirements for successful privacy achievement. Furthermore appropriate citizen trust in the government may not be present. The following sections outline the privacy requirements depicted in Figure 4 in more detail.

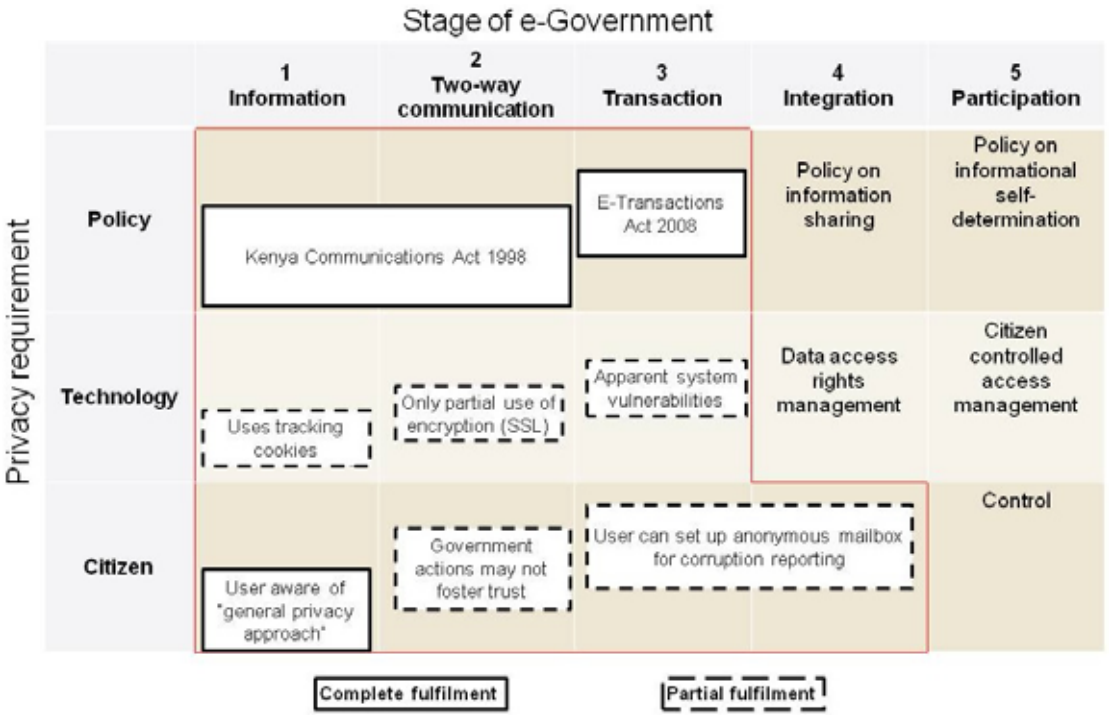

Figure 4: Assessment of Privacy Readiness of Kenya's e-Government Portal

Policy requirements

From the *Policy* perspective, regulations for protecting privacy in electronic communications and transactions are enacted and linked to the constitution. Kenya was an early adopter of ICT policy in Africa and has addressed the need for ICT policies since 1993 (Wanjiku, 2009). It began the process of breaking the government monopoly on communications in 1997 and formalized policy changes in 1998 with the Kenya Communications Act. This act included policies which supported the protection of citizen data, including requirements for informing users of electronic systems about what information is collected and for which purposes.

However, the Act included strong measures which were seen to limit the freedom of the press and freedom of expression (ibid). These measures were justified by the government as necessary to prevent racially-motivated retaliation by partisan, irresponsible media outlets. The government did have evidence to support this concern, given a history of such misuse by media outlets in both Kenya, and more notoriously in the lead-up to Rwanda's genocide. But the media has seen these measures as being excessive, and the public view of limiting media freedoms may not be conducive to citizen trust.

To spur development of further use of e-government and set a more solid base for electronic transactions the e-Transactions Act of 2008 was enacted by the Kenyan parliament in December 2008. Through this, international best practices, such as digital signatures and comprehensive data protection, were mandated for use in Kenyan e-government systems and processes. The e-Transactions Act also aimed to introduce compliance with the proposed East African cyber laws framework. Beyond this the Act has had a drawback in not addressing existing controversial measures for protecting privacy which allow for wide latitude when it comes to authorities acting to investigate and penalize misuse of information and communication technology (Wanjiku, 2009). Work on an amendment began and the private sector, civil society and the academic world were said to be consulted in the changes (ibid).

The revised e-Transactions Act did not include expected amendments to protect the media. However, it was generally embraced by the communications sector (Wanjiku, 2009). The provisions it introduced recognized cyber crime, electronic transactions, digital signatures, and set out universal funding – factors considered weak in the original. The combination of liberalization and control did facilitate growth of the telecommunications sector (ibid). This success may have helped minimize potential public concern.

Kenya's legislation goes a long way towards providing the necessary functions for citizen privacy but their application, as seen in the following section, may not be complete. This apparent gap along with evidence of government corruption can only hinder citizen trust in government initiatives. A level of critical mass of trust by the public is required for the adoption of government initiatives (Backus, 2001). This trust must promoted to the masses through awareness campaigns but also be demonstrated in reality.

Technology requirements

As noted above, some of Kenya's analysed e-government applications can be placed in the second maturity stage while the Tax Services and Corruption Reporting systems reach the third stage (Kenya, 2010a). Although policies mandate comprehensive measures regarding privacy protection, neither visitors to the e-government portal, nor two-way communication, nor transactions can be seen as sufficiently safe to use. The

web portal uses browser cookies which could potentially be used for collecting user information beyond what is necessary and even beyond the e-government portal. This could lead to user profiling. Secure (encrypted) communication channels do not exist for all applications which involve the transmission of citizen data. The more sensitive applications of tax filing and corruption reporting are nevertheless encrypted and can be considered safe in this respect. Still the tax system reveals vulnerabilities regarding access restrictions which allow for public access to the remote management interface (Kenya Revenue Authority, 2010). Although correct user name and password are still required to access the management interface, this could invite potential exploitation to obtain sensitive information. Hence, it can be suggested that the applications available on Kenya's e-government portal only partially fulfil the necessary requirements for technical maturity.

Citizen requirements

From the *Citizen* requirements perspective, the unfulfilled promises by the government regarding the e-Transactions Act could result in a major issue in trust and in turn disrupt the success of the portal and further e-government projects. Regarding awareness, only a general privacy statement is made (Kenya, 2010b). This is only partially relevant to the information to be collected and used, and more explicit policies are not provided for most sub-sites in the portal. For example, the policy states that information collected on the site will only be used to communicate with the user. Presumably, most of the sub-sites within the portal would required a more complex use of collected information; such as that required for applying for jobs or submitting tax returns.

An exception is Kenya's externally-developed and hosted corruption reporting system where the user is informed about which information is collected. This system stands out also because it extends to the fourth e-government maturity stage by allowing citizens to not only report corruption in person and face-to-face with authorities, but also in an anonymous way and beyond government agencies' boundaries.

However the success of this system and any other citizen-facing e-government project might be hampered by missing citizen trust in government. While the perspectives of actual users of the websites were not surveyed, there were characteristics of the sites

where trust by the user may not have been achieved. At an operational level, lack of awareness about the protection of collected data and no provision of secure channels may not satisfy discerning users. At a societal level, a widespread public perception of government corruption (Transparency International, 2009) and limitations to media freedoms (Wanjiku, 2009) may also harm trust in e-government systems.

The Kenyan constitution and the Communications Act of 1998 allow for restrictive control over media content and delivery by government authorities (Wanjiku, 2009). Government promised to ease these policies in the e-Transaction Act of 2008 but failure to deliver on these promises led to public protest and hence to trust issues which in turn could induce a negative citizen bias towards the use of e-government systems. This possible public relations issue for Kenya requires further analysis. However, it can be suggested that as long as the Kenyan government does not keep major information-related promises made to the citizens, missing trust constitutes an issue which might undermine citizen-facing e-government systems.

C3. Comparison of Case Examples

The two case examples outlined are not entirely similar e-government systems, and they must also be regarded as provisional given the relatively limited evidence base available. However, their presentation reveals the possibility to not only use the proposed framework for analysing individual e-government systems, but also for comparing them. While both countries have applications at the transaction stage, the framework suggests that Germany has met the necessary privacy requirements, while Kenya has only shown partial attainment. This is depicted in Figure 5. The comparison also shows that despite reaching the fourth stage of e-government with the Corruption Reporting system, not attaining all the necessary privacy readiness requirements – technical and particularly citizen requirements – could lead to a failure of this system. Of particular significance, basic trust in the government seems likely to be a major component for the success of citizen-facing e-government systems. Additionally, if the technical design is not perceived as being robust with adequate safeguards, citizen trust may be elusive (Gronlund, 2002). Perceived personal vulnerability may lead to resistance in citizen adoption of e-government. Thus technology or citizen factors alone can be critical success factors.

Summarizing the above, Kenya has instituted necessary policy measures but may not have met the technical requirements for successful privacy achievement. Additionally, although these policies are in place and linked to the constitution, the same constitution and government actions do not foster trust (Wanjiku, 2009). On the other hand, by sufficiently meeting all these successive requirements to the Transaction stage, Germany's Comprehensive Tax Administration system provides a more successful story which encourages the search for solutions to the issues faced by Kenya's e-government portal.

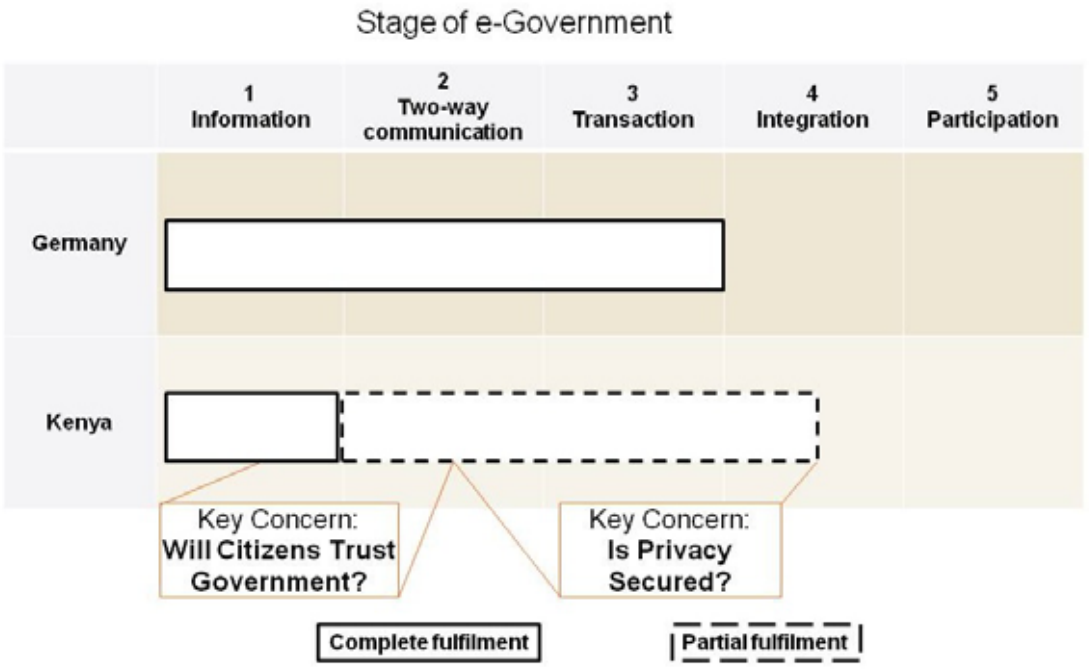

Figure 5: Comparison of Privacy Readiness Assessment – Germany vs. Kenya Cases

D. Conclusion: Implications for Researchers and Practitioners

Privacy is a critical issue underpinning the success and failure of e-government systems. Yet, to date, there has been a dearth of systematic frameworks by which to understand privacy, and by which to analyse the privacy readiness of e-government programmes and projects.

Reviewing the development of the proposed framework and its use for analysing and comparing the two case examples, we conclude that researchers and practitioners could use it for identifying and deriving root causes of major privacy-related issues in citizen-facing e-government systems. This is based on the framework considering three requirement categories applied to each maturity stage of e-government while integrating dependencies of requirement attainment between these stages. By providing this blueprint, zeroing-in on actual issues should be easier.

This facilitates on the one hand more targeted academic research, and on the other hand, higher efficiency in tackling design and implementation issues because the identification of privacy issues points fairly directly to recommendations for practice. This would most often be undertaken by applying the framework to individual e-government programmes and projects. However, here we have shown the applicability of the framework to a comparative – potentially even benchmarking – approach.

Of course the two selected settings here were very different and the evidence base for this short paper necessarily limited. Nonetheless, the potential is clear for a comparative application to transfer knowledge and practice about privacy from one project to another. Via this new framework, the academic debate about privacy as a success factor for e-government could target discovery and transfer of knowledge in a more structured way while e-government projects could benefit from more targeted use of this knowledge to deliver successful practice.

References

Backus, M. (2001) *E-Governance and Developing Countries*, International Institute for Communication and Development (IICD) [Online], Available: http://www.iicd.org/files/report3.doc

Belanger, F. and Hiller, J. (2006) A framework for e-government: privacy implications, *Business Process Management Journal*, 12(1), pp. 48-60

Choudrie, J., Olla, P. and Raza, S. (2009) Exploring the issues of security, privacy and trust in e-government: UK citizen's perspective, *AMCIS 2009 Proceedings*, Paper 347.

Culnan, M. (2000) Protecting privacy online: Is self-regulation working?, *Journal of Public Policy & Marketing*, 19(1), pp. 20-26

El Kiki, T. and Lawrence, E. (2006) Government as a mobile enterprise: real-time, ubiquitous government, *Proceedings of the Third International Conference on Information Technology: New Generations (ITNG'06)*, pp. 320-327

Elster (2010a) *ELSTER: Project, English Information*, Bavarian State Office for Taxes [Bayerisches Landesamt für Steuern] [Online], Available: https://www.elster.de/pro_infoeng.php

Elster (2010b) *ELSTER: Statistical Information [ELSTER: Statistische Zahlen]*, Bavarian State Office for Taxes [Bayerisches Landesamt für Steuern] [Online], Available: https://www.elster.de/elster_stat_nw.php

Elster (2010c) *ELSTER: Privacy Protection Statement [ELSTER: Datenschutzhinweise]*, Bavarian State Office for Taxes [Bayerisches Landesamt für Steuern] [Online], Available: https://www.elster.de/datenschutz.php

Federal Office of Information and Security (2009) *Federal Office for Information Security Certifies ELSTER [BSI zertifiziert ELSTER]*, Federal Office for Information Security [Bundesamt für Sicherheit in der Informationstechnik] [Online], Available: https://www.bsi.bund.de/cln_183/ContentBSI/Presse/Pressearchiv/Kurzmit2009/180209Elster.html

Gronlund, A. (2002) *Electronic Government: Design, Applications and Management*, IGI Global, London

Holvast, J. (2009) History of privacy, in *The History of Information Security: A Comprehensive Handbook*, K. de Leeuw, K. and J. Bergstra (eds.), pp. 737-770

Kenya (2010a) *Welcome to Kenya E-Government*, Directorate of e-Government [Online], Available: http://www.e-government.go.ke

Kenya (2010b) *Privacy Statement*, Directorate of e-Government [Online], Available: http://www.e-government.go.ke/index.php?option=com_content&view=article&id=87&Itemid=29

Kenya Revenue Authority (2010) *Kenya Revenue Authority - Integrated Tax Management System*, Kenya Revenue Authority [Online], Available: https://mapato1.kra.go.ke/itms/.

Langenderfer, J. and Miyazaki, A. (2009) Privacy in the information economy, *Journal of Consumer Affairs*, 43(3), pp. 380-388

LaRose, R. and Rifon, N. (2007) Promoting i-safety: effects of privacy warnings and privacy seals on risk assessment and online privacy behavior, *Journal of Consumer Affairs*, 41(1), pp. 127-149

Laudon, K. and Laudon, J. (2009) *Management Information Systems*, Prentice Hall, 11th revised edition, Upper Saddle River, N.J.

Orwell, G. (1949) *Nineteen Eighty-Four*. Signet, New York, N.Y.

Solove, D. (2004) *The Digital Person: Technology and Privacy in the Information Age*, NYU Press, New York, N.Y.

Symonds, M. (2000) Government and the internet: no gain without pain, *The Economist*, Vol. 355, pp. 9-14

Transparency International (2009) *Corruption Perceptions Index 2009*, Transparency International [Online], Available: http://www.transparency.org/policy_research/surveys_indices/cpi/2009/

Wanjiku, R. (2009) *Kenya Communications Amendment Act (2009) - Progressive or Retrogressive?*, Association for Progressive Communications [Online], Available: http://www.apc.org/en/system/files/CICEWAKenya20090908_EN.pdf